Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) An automated encryption system for encrypting an electronic message from a sender to a recipient comprising:

a computer readable medium in communications with a sender's e-mail client;

~~a network port in communication with said computer readable medium for accessing a set of public key data having a public key associated with the recipient; and,~~

a set of encrypted private keys associated with senders' ID's and passwords stored in said computer readable medium;

a set of computer readable encryption instructions embodied in said computer readable medium for[[:]] receiving said electronic message from said e-mail client that is created by the sender and addressed to the recipient having the sender's ID and password, attempting to decrypt the sender's private key according to said sender's ID and password, if the sender's private key is successfully decrypted, attempting to retrieve~~ing~~ said recipient's public key ~~associated with the recipient~~ from said ~~public key data via said network connection~~ computer readable medium, the sender's private key is successfully decrypted, but the recipient's public key is not located in said computer readable medium attempting to retrieve the recipient's public key from a PKI server in communications with said computer readable medium if said recipient's public key is located, encrypting said

electronic message according to said recipient's public key ~~associated with the recipient~~, ~~and~~ forwarding said encrypted message to the recipient for subsequent retrieval so that the electronic message is automatically encrypted and delivered to the recipient without the need for the email client to retrieve the recipient's public key or encrypt the message.

2. (Currently Amended) The system of claim 1 ~~including:~~ wherein

~~a set of private key data embodied in said computer readable medium having a private key associated with the sender; and,~~ said set of computer readable encryption instructions include instructions for[[:]] retrieving said private key associated with the sender from said set of private key data and digitally signing said electronic message from the sender according to said private key associated with the sender so that the recipient can verify the authenticity of said electronic message.

3. (Currently Amended) The system of claim 1 ~~including~~ wherein:

~~a set of private key data contained within said computer readable medium having a private key associated with the sender; and,~~

~~a set~~ said set of computer readable ~~access~~ instructions include instructions that if the sender's private key is successfully decrypted but the recipient's public key is not located on said PKI server, attempting to retrieve the recipient's public key from a certificate authority in communications with said computer readable medium. ~~embodied in said computer readable medium for: receiving an access attempt input from the sender, retrieving said private key associated with the sender from said set of private data, validating said access attempt input according to said private key to determine whether a~~

~~valid access attempt input has been provided, and encrypting said electronic message according to said public key if said access attempt input is valid so that only senders with valid access attempt inputs may send encrypted messages.~~

4-6. (Canceled)

7. (Currently Amended) The system of claim 1 including:

~~a set of encrypted private key data contained within said computer readable medium; and,~~

a set of computer readable key maintenance instruction embodied within said computer readable medium for[[:]] creating a key pair having said at least one public key associated with the sender and a private key associated with said public key and the sender, storing said public key within said set of public key data so that said public key associated with the sender is available for retrieval, receiving a password from the sender, encrypting said private key according to said password, storing said encrypted private key within said private key data so that the sender can retrieve said private key for decrypting message sent to the sender, and[[,]] deleting said key pair to prevent the sender from decrypting encrypted messages so that an automated key management system is provided for automatically managing key pairs for senders.

8. (Currently Amended) An automated encryption system for decrypting an electronic message from a sender to a recipient comprising:

a computer readable medium <u>in communication with a sender's mail server</u>;

~~a set of private key data embodied within said computer readable medium having a~~

~~private key associated with the recipient; and,~~

a set of computer readable decryption instructions embodied within said computer readable medium for receiving a recipient's access attempt from a client representing an attempt to retrieve a message sent from the sender to the recipient having recipient's ID and password, attempting to decrypt sender's private key according to recipient's ID and password, if the sender's private key is decrypted, decrypting said message with said sender's private key and forwarding said decrypted message to the recipient. ~~said electronic message from the sender to the recipient, retrieving said private key associated with the recipient from said set of private key data, decrypting said electronic message according to said private key, and, providing said decrypted message to the recipient so that the recipient automatically retrieves and decrypts an electronic encrypted message without manually managing private keys.~~

9. (Currently Amended) The system of claim 8 wherein ~~including~~:

~~a network port in communication with said computer readable medium for accessing a set of public key data having a public key associated with the sender; and,~~

~~a set~~ said set of computer readable ~~message verification~~ instructions include instructions for ~~embodied within said computer readable medium for receiving said encrypted message having a digital signature associated with the sender,~~ retrieving said public key associated from the sender, ~~sender from said digital signature,~~ attempting to validate ~~validating~~ said electronic message according ~~to said~~ to a digital signature associated with said digital signature, ~~to provide validation information,~~ and providing the

~~resulting~~ validation results ~~information~~ to the recipient so that the recipient can be notified as to the authenticity of the ~~received encrypted~~ message.

10-12 (Canceled)

13. (Currently Amended): A ~~computerized system~~ method for encrypting an electronic message from a sender to a recipient comprising the steps of:

~~a computer readable medium;~~

~~a means for~~ receiving an electronic message from an email client that is created by a sender and addressed to a recipient ~~embodied in said computer readable medium~~;

~~a means for obtaining a public key associated with the recipient;~~

attempting to decrypt the sender's private key according to said sender's ID and password;

retrieving said recipient's public key from a computer readable medium if said sender's private key is successfully decrypted;

~~a means for~~ encrypting said electronic message according to said recipient's public key; and,

~~a means for~~ forwarding said encrypted electronic message to the recipient for subsequent ~~decryption and~~ retrieval without the need for the sender's email client to retrieve the sender's public key or encrypt said message.

14. (Currently Amended): The ~~system~~ method of claim 13 including the steps of:

[[an]] retrieving an encrypted private key associated with the sender encrypted according to the sender's [[a]] password ~~supplied to the sender and contained within said~~

~~computer readable medium~~;

~~a means for~~ receiving an access attempt from the sender; and,

~~a means for~~ validating said access attempt according to said encrypted private key so that said electronic message is not encrypted unless said access attempt is valid.

15. (Currently Amended): The ~~system~~ method of claim 13 including the steps of:

~~a means for~~ informing the sender that said public key associated with the recipient cannot be found so that electronic message cannot be encrypted; and,

~~a means for~~ sending said electronic message to the recipient unencrypted.

16. (Currently Amended) The ~~system~~ method of claim 13 including the steps of:

~~a computer readable medium;~~

~~a means for~~ receiving an encrypted electronic message from the sender addressed to the recipient;

~~a means for~~ obtaining a private key associated with the recipient; and,

~~a means for~~ decrypting said encrypted electronic message from the sender to the recipient so that the recipient can receive and decrypt an encrypted message.

17. (Currently Amended): The ~~system~~ method of claim 13 including the steps of signing said electronic message with a digital signature associated with the sender. ~~:~~

~~a digital signature associated with the sender contained within said computer readable medium; and,~~

~~a means for signing said electronic message with said digital signature.~~

18. (Currently Amended): The ~~system~~ method of claim 13 including the steps of:

~~a means for~~ receiving an electronic message having a digital signature associated with the sender; and,

~~a means for~~ verifying the authenticity of said electronic message according to said digital signature so that the recipient is ensured that said electronic message truly originates from the sender.

19. (Canceled)